10. COE Online Services

The DII COE provides a comprehensive set of services to assist in

- creating segments,
- tracking and managing submitted segments,
- tracking system trouble reports,
- distributing technical information and documents,
- communicating project-related information,
- distributing COE products to segment developers, and
- distributing COE-based systems to operational sites.

These services are provided by a Software Distribution Management System (SDMS) and a COE Information Server (CINFO). The SDMS is an online software repository for receiving submitted segments, and for distributing them electronically, and for synchronizing repositories at mirror sites. The CINFO is used to disseminate project-related information including schedules and documentation. With appropriate restrictions, SDMS and CINFO services are available to segment developers, program managers, site administrators, services and agencies, and program sponsors.

Several network technologies are used to implement COE online services.

World-Wide-Web (WWW)	Access to catalogs, segments, plans, documents, etc. is provided via a WWW server. It is the standard interface to both SDMS and CINFO. Users will require a Hypertext Markup Language (HTML) browser such as Mosaic, Netscape, or Microsoft's MSN to access the WWW server.
Internet News	An Internet news server is used to manage newsgroups for to the COE and COE-based systems. Such groups include technical discussions related to COE architecture, available tools, and standards.
anonymous ftp	Anonymous ftp servers are used to provide rapid dissemination of segments to operational sites. Sites may receive segments in either a "push" or a "pull" mode.
electronic mail	Automatic notification of key events (segment in test, segment ready for distribution, etc.) trouble reports, and meeting notices is done via electronic mail.

This approach provides several benefits to COE-based systems:

- Facilitates software and data reuse (e.g., segment reuse)
- Identifies available segments through a segment catalog
- Provides online configuration management
- Automates several aspects of the integration process
- Provides electronic notification of segment status to management
- Improves communications between segment developers
- Provides a centralized electronic distribution facility
- Separates classified or sensitive information from information suitable for general dissemination

Appendix D provides more information on how to access the COE online services described in this chapter.

10.1 Security Features

COE online services are separated onto a classified and an unclassified system. The systems, whether classified or unclassified, use a secure operating system, database, and network software. Auditing is enabled to record system access and to record other security-relevant operations. Additional security features are implemented to

- ensure software integrity,
- prevent interception or eavesdropping on data transmissions, and
- ensure separation of classified versus unclassified information, segments, and data.

The classified and unclassified components reside on physically distinct computer systems separated by an air gap. The unclassified system is available via Internet and is generally available to any interested party. The classified system is accessible only via SIPRNET, and only by authorized users.

Unauthorized access to the system is prevented through a layered approach. Firewalls are implemented as the first layer of protection. Secure routers provide IP address filtering and port access to limit access only to authorized workstations. Features are also implemented to restrict services that can be requested or granted to further protect the system from unauthorized access.

User authentication is based on a combination of a manual registration process, an authorized IP address, and password protection. Passwords are required to initially log onto the system, but are further required to log into the software repository and to access browser services.

Public key encryption is used to protect segments in the software repository. Encryption and compression are both used to protect data during transmission over the network to prevent unauthorized modifications.

Certain information, such as system problem reports or project status, is not necessarily classified. However, such information is still sensitive and needs to be controlled. Public and private views are implemented to provide this measure of protection.

Further discussion of security features is beyond the scope of this document.

10.2 Software Distribution Management System (SDMS)

SDMS is the DII software repository, and it is used to store and disseminate COE and COE-related products. SDMS is accessible only from SIPRNET. Segments, technical documentation, APIs, the COE developer's toolkit, and segment abstracts are also stored in the repository, but as appropriate, they are mirrored on the unclassified Internet set for access by the general community.

Segments are sent electronically to the DISA Operational Support Facility (OSF) through the `submit` program. Segments may also be sent to the OSF via tape. This is necessary to accommodate large segments (such as database segments) or classified segments. Segments are compressed to reduce transmission time, and encrypted to provide security. A daemon running on a system at the OSF receives the segment and places it into a protected directory until it is tested for conformance and to ensure that it is an authorized segment. Only then is the segment actually checked into the SDMS. This process is described in more detail in Chapter 3.

Segments are retrieved from the SDMS in a similar way. As segments are approved for release, they are placed in a protected directory that is accessible via an anonymous ftp, or through a network browser.

Developers who desire SDMS access must request access from DISA through their appropriate government program sponsor. Those without SIPRNET access may request COE products, such as the developer's toolkit, on tape media.

Distribution of COE-based systems to operational sites also uses the SDMS. Site administrators must request access from DISA through their appropriate government channels.

10.3 COE Information Server (CINFO)

The COE information server is used to disseminate information to the at-large COE community. The information server provides the following types of information:

- general product information
- meeting minutes
- briefings
- segment descriptions
- user documentation
- programmatic documentation
- problem reports.

An unclassified WWW home page available via the Internet provides access only to non-sensitive general information from these categories. The classified WWW home page is available only on SIPRNET and includes a list of all available segments, segment version and patch information, information on upcoming system changes, and special installation instructions.

All information posted on the information server requires prior approval by the DISA Engineering Office. Information to be posted must be submitted to the engineering office by the appropriate service/agency representative.

10.4 Mirror Sites

Project managers for COE-based systems will often have their own Software Support Activity (SSA) and procedures for configuration management, development, and project communication. Services and government agencies may wish to implement the COE online services at their own selected sites to more directly support their program. Such SSA sites are called *mirror sites*. A mirror site contains a copy of the SDMS that is updated on a periodic basis (e.g., daily, weekly).

Mirror sites have all of the same capabilities as the central DISA site, subject to three restrictions:

1. Mirror sites are not allowed to submit COE-component segments to a mirror site SDMS. This ensures centralized configuration management of the COE through the DII COE SSA.

2. Mission-area segments that are part of a COE-based system being developed in cooperation with DISA (e.g., GCCS, GCSS) may be provisionally submitted to a mirror site SDMS.

3. Segments with APIs for which a mirror site is responsible may be provisionally submitted to the mirror site SDMS.

Submission of COE-component segments or mission-application segments for DISA COE-based systems is considered provisional until formally accepted by the DII COE SSA. These restrictions are required in order to avoid configuration management problems.